Morning Shift attendance || 10-06-2023

Hi All,

All are present in the shift except below,

Hello CSOC Team , kindly confirm your availability for Night Shift today along with WFO status.

Hello CSOC Team , As per the instructions , Kindly work on pending cases more than 2 days and update on closure of this cases till 12 PM .

Kindly Update here the Tickets and Analysis for TCS TIP report

If we didn’t receive any update from your side , same will be updated in the sheet .
Any doubts / concerns regarding cases closure can be discussed .

Hi Team, facing slowness issue in demisto

Break timing

Manage Shift handling Incident in Demisto

2. Reports and GRA cases Assignments

3. Critical cases analysis from Analysts

4. IP Blocking mails to Firewall and NOC team

5. Raise RFC for domain blocking on other proxies

6. Consoles commands to be checked at shift end

7. Commands for checking Console Alive status

8. Checking Incidents for Lateral movement alert

9. Sharing Shift status mail at the end

10. Suggestions for whitelist/finetune alerts

11. Inform about critical alerts to CSOC Manager

12. Help associates at any point of request

13. Approve azure access requests of the associates

Daily Status Updates 21st July 2023 Morning Shift

Hi All,

Please find the below detail.

1. All incidents are assigned in shift from 2:00 pm to 9:30 pm.
2. All offenses are assigned & closed in the SIEM tool in a shift from 2:00 pm to 9:30 pm.
3. All mailboxes are monitored in shift from 2:00 pm to 9:30 pm.
4. Checked the logs for account name oth.kroll - No event observed.
5. No new files were detected in EDR Tool.
6. Checked all GRA commands till 9:30 pm no anomalies observed.
7. No detection was observed for spoolsv.exe
8. 4 Phishing email was received during the shift from 2:00 pm to 9:30 pm.
9. No host is contained or lifted from containment in a shift from 2:00 pm to 9:30 pm.
10. No tickets having parent ticket age older than 1 day found.
11. No response SLA was missed during the shift from 2:00 pm to 9:30 pm.
12. 0 alert was observed in Crowdstrike PCI/India Cloud Tenant.
13. 0 alert found in CrowdStrike GNDM Tenant.
14. If any alerts are received from IP 54.217.50.18, 50.208.202.111, and 52.49.144.209 inform Yogesh/Nimisha --> **No alerts received**.
15. 0 risky users mail assigned in the shift.
16. Please notify Nimisha/Yogesh if any alerts are received from User: 2346248 Host: 01VD0076945 Email: jain.mailto:ayush11@tcs.com and ayush11@tcs.com --> **No alerts received**
17. No discrepancies were found in alert increase and decrease.
18. Monitor this server “CDCTPPTLAB15” & if any alert triggered inform Yogesh & Nimisha --> **No alerts received**

TABLE

Analysis

Please find the below detail.

1. All Alerts are assigned in the shift from 6:30 am to 2:00 pm.
2. All offenses are assigned & closed in the SIEM tool in the shift from 6:30 am to 2:00 pm
3. All mailboxes are monitored in shift from 6:30 am to 2:00 pm
4. Checked the logs for account name oth.kroll - No event observed.
5. No new file detected in EDR Tool.
6. Checked all GRA commands till 2:00 AM , No anomaly was observed.
7. No detection was observed for spoolsv.exe
8. 0 Phishing email alerts were received during the shift.
9. No host was contained, and No host was lifted from containment in the shift.
10. No tickets having parent ticket age older than 1 day found.
11. No response SLAs were breached during the shift.
12. No critical alert was found in CrowdStrike India Cloud Tenant.
13. No alert was found in CrowdStrike PCI Tenant.
14. No alert found in CrowdStrike GNDM Tenant.
15. If any alerts are received from IP 54.217.50.18, 50.208.202.111, and 52.49.144.209 inform Yogesh/Nimisha - No alerts received
16. Please notify Nimisha/Yogesh if any alerts are received from user "2346248", Host "01VD0076945", Email "jain. [mailto:ayush11@tcs.com"--]ayush11 @tcs.com"-- - No alerts received
17. 0 risky users mail assigned in the shift.
18. Monitor this server "CDCTPPTLAB15" & if any alert triggered inform Yogesh & Nimisha. (No alert Received)
19. No discrepancies found in alert increase and decrease.
20. No alerts received from XDR , verified the same manually.

PFB reports worked on:

- RE: RSAOTP:Multiple login attempts from different source IP addresses Dec 8, 2023, 9:50:59 PM
- RE: Apache Log4J Vulnerability denied communication Dec 9, 2023, 5:21:11 AM
- RE: Recon_Activity_IPS_portscan Dec 9, 2023, 5:13:26 AM
- RE: Report:Azure:Suspicious Logins from Powershell Dec 9, 2023, 4:31:23 AM
- RE: Recorded_Future_Inbound_Communication
- RE: CISCO DUO REPORTS
- RE: Windows_Failed_Login_attempts_eventcount_morethan_50 Dec 9, 2023, 1:08:41 PM
- RE: RSAOTP:Multiple Failed Login attempts

Please take care of the below reports:

- RE: RSAOTP:Multiple login attempts from different source IP addresses Dec 8, 2023, 9:50:59 PM
- RE: Apache Log4J Vulnerability denied communication Dec 9, 2023, 5:21:11 AM
- RE: Recon_Activity_IPS_portscan Dec 9, 2023, 5:13:26 AM
- RE: Report:Azure:Suspicious Logins from Powershell Dec 9, 2023, 4:31:23 AM

- RE: Recorded_Future_Inbound_Communication
- RE: CISCO DUO REPORTS
- RE: Windows_Failed_Login_attempts_eventcount_morethan_50 Dec 9, 2023, 1:08:41 PM
- RE: RSAOTP:Multiple Failed Login attempts

Please check for new reports Generated .

IOC’s to be blocked :

None

CrowdStrike India Cloud Tenant Cases Update:

No cases

CrowdStrike PCI Tenant Cases Update:

No cases

CrowdStrike GNDM Cases Update:

No cases

Previous Shift Handover Cases Update :

- Falcon Overwatch via Suspicious Activity_IBEXTOOLS5GC4_Network Isolated -- Reminder sent
- Hackvist Indonesia IOC -- Worked on IOCs

Please take care of the handover cases below :

- Falcon Overwatch via Suspicious Activity_IBEXTOOLS5GC4_Network Isolated – check with vaithi sir once received update on same -- Follow up

team share IOC for blocking /HO
and any host contained / uncontained during the shift

UPDATE TO MANAGER'S

There were No critical Cases triggered in Morning Shift today .

Previous Shift Handover Cases Update :

- Falcon Overwatch via Suspicious Activity_IBEXTOOLS5GC4_Network Isolated – check with vaithi sir once received update on same - follow up

Please take care of the handover cases below :

- Access Attempt to login || 10.101.20.100 - Take follow up
- Credential Scanning (Active Directory) || INBLRANCPPSN -- Mail drafted just check details and send

Pending case update :

No repetitive alerts observed and No detection SLA missed !

following are cases raised for reports assigned to associates and there are no cases pending to be raised

Malicious IPs to block – 26th June 2023 Night Shift

Dear Team ,

Please block below mentioned IP as they are categorized as malicious. Kindly confirm us once blocking is done at your end.

Note: Mentioned IPs will be blocked on PaloAlto FW through demisto.

Report to send autobot for discrepancy

All Domains:Group member Details

Hello CSOC Team , Kindly Work on this report and Create demisto ID individually and update me analysis by 1pm . Need to share this analysis to CSOC managers , Hence please work accordingly and let me know in case of Issues / Doubts .